UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/672,796	09/26/2003	Andrew Morgan	TRAN-P162	9469

7590 08/22/2007

WAGNER, MURABITO & HAO LLP
Third Floor
Two North Market Street
San Jose, CA 95113

EXAMINER	
PICH, PONNOREAY	
ART UNIT	**PAPER NUMBER**
2135	

MAIL DATE	DELIVERY MODE
08/22/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/672,796	MORGAN ET AL.	
	Examiner	Art Unit	
	Ponnoreay Pich	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 6/4/07.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-26 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-26 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-26 are pending.

Response to Arguments

Applicant's arguments were fully considered, but were not persuasive. Applicant argues that Okada does not teach the limitation of "wherein said digital secret is internally accessible only within said processor" as recited in claim 1 and as similarly found in the other independent claims. The examiner respectfully disagrees.

Claim 1 will be used as a representative claim in the discussion. As explained in the rejection of claim 1, any of the following which is disclosed by Okada can be considered the claimed digital secret: the secret key used by the processor to encrypt the processor ID and used to decrypt the "Key" sent to from the software supplier (col 10, lines 15-18 and 46-49); the private key of the processor which is used to decrypt the "Key" sent to from the software supplier (col 12, lines 15-19); or the processor ID 16 (col 8, lines 1-4).

If one were to consider the secret key used to by the processor as the claimed digital secret, then the secret key meets the limitation of being internally accessible only within said processor because no other component of computer system 200 as seen in Figure 1 accesses this secret key which is stored only in the processor 100 (col 11, lines 8-10). It is true that the software supplier also has a copy of the secret key to decrypt the processor ID sent to it by the computer 200 and to encrypt a "Key" which the software supplier then sends to computer 200, however, access to the secret key by the software supplier is done externally to system 200. As such, when considering

components internal to system 200, since access to the secret key is only done by and within processor 100, the limitation is met.

Note that Okada's invention has the option of using either a secret key to encrypt and decrypt messages sent between computer 100 and the software supplier or it could use an asymmetric key system. In the case that an asymmetric key system is used, one can consider the private key of the public/private key pair as meeting the claimed limitation. Okada discloses that part of the procedure of installing software includes encrypting the processor ID and a public key stored in processor 100 using the public key of the software supplier and sending the result to the software supplier (col 11, lines 49-56). The software supplier decrypts the message sent by computer 200 using its own private key and sends a "Key" back to the system which was encrypted using the public key of the processor 100 (col 11, lines 59-67). Processor 100 uses its stored private key to decrypt the "Key" sent by the software supplier (col 12, lines 15-19). A person of ordinary skill in the art should understand that in an asymmetric key system, there are two key values used—a private key and a public key. The public key is freely distributed to other parties while the private key is never distributed. As such, because the processor's private key is stored only in the processor 100, is never distributed outside the processor, and is accessible only by the processor 100, the limitation that the processor's private key, i.e. the claimed digital secret, is internally accessibly only within the processor is met.

If one were to consider the processor ID as being the claimed digital secret, it meets the limitation because the only way to gain access to the processor ID is for the

processor to provide it since the processor ID is stored internally within the processor. Further, no other component of system 200 is ever disclosed by Okada as accessing the processor ID except those which are internal to and part of processor 100.

On page 12 of the remarks submitted, applicant requested support for the taking of official notice that "wherein said digital secret and said internal memory are integrated with said cryptography engine to facilitate communication without requiring a bus and which is not susceptible to malicious attack" is well known in the art at the time applicant's invention was made. In response, the examiner provides Easter et al (US 5,563,950) and Klein (US 7,096,370) as supporting documents.

Easter discloses a cryptography engine (Fig 2, item 63) having a digital secret, i.e. key in key array 25, and an internal memory (Fig 2, key array 25) wherein the key and key array are integrated with cryptography engine 63 (Fig 2, item 63 and col 4, lines 49-65). Since the digital secret and internal memory is integrated as part of the cryptography engine 63, no bus is required for communication since the engine is in essence communicating with itself. Easter also discloses that there is not way to discover the secret key stored in the integrated circuit 63 except for destruction of the chip, thus the cryptography engine 63 is not susceptible to malicious attack (col 3, lines 39-52). As such, Easter provides support for the official notice.

Klein also provides support for the official notice. Klein discloses of a logic circuit 50 (see Figure 3), which is a cryptography engine having an integrated digital secret (either key 66 or hardware identifier 64) and an integrated internal memory, i.e. the memory used to store key 66 and hardware identifier 64. Because the key and internal

memory of logic circuit 50 is integrated within the logic circuit, no bus is required for communication since it is communicating with itself and it is not susceptible to malicious attack since the key never leaves logic circuit 50.

Applicant's remaining remarks are directed towards dependency. However, because Okada does in fact disclose the limitation under contention, these dependent claims are also not allowable.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-7, 9-11, 14, 21, and 23-24 are rejected under 35 U.S.C. 102(e) as being anticipated by Okada (US 6,704,872).

Claim 1:

Okada discloses:

1. A digital secret that comprises a secret key used in a key-based cryptographic process, wherein said digital secret is internally accessible only within said processor (col 11, lines 8-10, 23-28; col 9, lines 31-36; and col 12, lines 15-19,

60-65). *The secret key and the private key of the processor stored in the processor can both be considered the digital secret or at least part of the digital secret. The processor id 16 can also be considered part of the digital secret or by itself the digital secret since an authenticated processor id allows a program to be executed by a processor (col 12, lines 20-30), thus the processor id acts as a "secret key" for allowing program execution.*

2. A cryptographic engine for performing said key-based cryptographic process internally within said processor, said cryptography engine coupled to said digital secret (Fig 1, item 17; Fig 5, item 17; col 10, lines 15-19 and lines 46-49).
3. Internal memory, i.e. ROM 14 and registers of processor 100, coupled to said cryptography engine for supporting said key-based cryptographic process (Fig 1, item 14; Fig 5, item 14; col 8, lines 26-35; col 11, lines 1-22; and col 12, lines 35-59). *Note the memory which is used to store either the secret key or the public/private key pair used by the encryption/decryption unit 17 can also be considered the internal memory or part of the internal memory.*

Claim 2:

The limitation of an internal bus for facilitating secure communication between said cryptography engine, said digital secret, and said internal memory within said processor is inherent to Okada's invention because Okada discloses that the authentication procedure according to his invention is executed totally invisibly from external program (col 11, lines 23-28). This means that for each of the functional units seen in processor 100 of Figures 1 and 5 to be able to perform authentication via the

program codes discussed by Okada (col 11, lines 1-22 and col 12, lines 35-59), an internal bus is needed to connect each of these functional units to facilitate secure communication between the units so that an external program cannot observe what is happening within the processor 100.

Claim 3:

Okada discloses wherein said digital secret is securely confined within said processor (col 11, lines 23-28 and col 12, lines 60-65). An external program cannot view the authentication procedure by processor 100 which uses either the secret key or the private key, thus the key, i.e. digital secret, is securely confined within said processor.

Claim 4:

Okada further discloses wherein said internal memory, i.e. ROM 14 and registers of processor 100, comprises: microcode for implementing said key-based cryptographic process on data within said processor (col 8, lines 26-35).

Claim 5:

Okada further discloses wherein said internal memory securely stores intermediate data created within said key-based cryptographic process (col 8, lines 26-35; col 11, lines 1-29; and col 12, lines 35-59).

The cited section in column 8 discusses how ROM 14 stores microcode executed by the processor and data is written to the register of the processor. The microcodes for authentication in columns 11 and 12 have intermediate data which are stored securely such that an external program cannot see what is happening in the processor.

Claim 6:

Okada further discloses a cryptography unit comprising a functional unit within said processor for securely executing said key-based cryptographic process internally within said processor (Figures 1 and 5, item 17), wherein said cryptography unit comprises: said digital secret; said cryptography engine; and said internal memory (col 11, lines 1-28 and col 12, lines 15-24, 35-65).

Claim 7:

Okada further discloses wherein said key-based cryptographic process comprises: a key-based encryption process; and a key based decryption process (col 10, lines 15-19, 46-49; col 11, lines 49-54; and col 12, lines 15-19).

Claim 9:

Okada further discloses wherein said digital secret is unique to said processor and is permanently and physically manifested within said processor (col 11, lines 8-10, 23-28; col 9, lines 31-36; and col 12, lines 15-19, 60-65). The examiner is considering the digital secret as comprising the processor id and/or either the secret key or private key in the cited sections. Okada discusses that the processor id is unique to the processor, is assigned during manufacturing, and written to non-volatile memory (col 6, lines 39-42 and col 9, lines 31-36). A digital secret comprising a portion that is unique is also unique. The secret key and private key is also discussed in the cited sections as being stored in the processor, thus the digital secret being a combination of the processor id and/or processor key is permanently and physically manifested in the processor since storage is via use of non-volatile memory.

Claim 10:

Claim 10 is a combination of what is recited in claims 1 and 6 and is rejected for the same reasons given therein.

Claim 11:

Claim 11 is similar to what is recited in claim 7 and is rejected for the same reasons given therein.

Claim 14:

Claim 14 recites limitations similar to what is recited in claim 9 and is rejected for the same reasons given therein.

Claim 21:

Okada disclose:

1. A secure hardware environment providing core processing functionality (Figures 1 and 5, item 100), wherein said secure hardware environment comprises:
    a. A secure cryptography unit (Figures 1 and 5, item 17), wherein said cryptography unit internally provides secure cryptographic capabilities as a functional unit within said secure hardware environment (col 9, lines 37-52).

Claim 23:

Claim 23 recites limitations substantially similar to what is recited in claim 1 and is rejected for the same reasons given therein.

Claim 24:

Claim 24 recites limitations substantially similar to what is recited in claim 5 and is rejected for the same reasons given therein.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 8, 13, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okada (US 6,704,872) in view of Fahrny (US 2004/0098591).

Claim 8:

Okada further discloses a secure hardware environment providing core processing functionality (Figures 1 and 5, item 100; col 11, lines 23-28; and col 12, lines 60-65).

Okada does not explicitly disclose secure software environment coupled to said secure hardware environment, said secure software environment generating executable instructions that are sent to said secure hardware environment for processing, said secure hardware environment in combination with said secure software environment providing processor capability, and wherein said secure hardware environment is accessible only through said secure software environment.

However, Fahrny discloses a secure software environment coupled to a secure hardware environment (paragraphs 10 and 26), said secure software environment

generating executable instructions that are sent to said secure hardware environment for processing (Fig 1 and paragraphs 26-28), said secure hardware environment in combination with said secure software environment providing processor capability, and wherein said secure hardware environment is accessible only through said secure software environment (Fig 1, item 16 and paragraphs 28 and 31).

Note in the cited section of Fahrny that a secure hardware (Fig 1, item 16) authenticates software objects, including a trusted operating system at initialization. Access to any items in the secure hardware has to be done via an authenticated software object, i.e. trusted OS. The combination of authenticated software objects, i.e. secure software environment, along with the secure hardware (Fig 1, item 16) provides processor capability.

At the time applicant's invention was made, it would have been obvious to one of ordinary skill in the art to modify Okada's invention according to the limitations recited in claim 8 in light of Fahrny's teachings. One skilled would have been motivated to do so because Fahrny's teachings would further protect data within a secure hardware, i.e. Okada's secure processor 100, by authenticating software objects prior to allowing the software object access to any data in the secure hardware (Fahrny: paragraph 10). Note that this would further Okada's goal of providing an improved technology to prevent illegal execution of a program which can not be externally monitored or modified (col 3, lines 39-44). By controlling which programs are allowed access to the data stored in Okada's processor via Fahrny's teachings, one is more likely to prevent illegal

program execution and prevent external monitoring of what is happening inside the processor.

Claim 13:

Claim 13 recites limitations similar to what is recited in claim 8 and is rejected for the same reasons given therein.

Claim 22:

Claim 22 recites limitations similar to what is recited in claim 8 and is rejected for the same reasons given therein.

Claim 12 is rejected under 35 U.S.C. 103(a) as being unpatentable over Okada (US 6,704,872) in view of Cmelik et al (US 6,031,992).

Claim 12:

Okada does not explicitly disclose wherein said processor comprises a very long instruction word processor (VLIW) processor. However, Cmelik discloses the limitation (col 8, lines 51-65). At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Okada's invention according to the limitations recited in claim 12 in light of Cmelik's teachings. One skilled would have been motivated to dos o because use of a VLIW processor would increase the speed of processor execution by eliminating the need for each steps each time the target instruction is encountered (Cmelik: col 9, lines 51-65).

Claims 15-17 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okada (US 6,704,872) in view of Balard et al (US 2004/0025036).

Claim 15:

As per claim 15, Okada does not explicitly disclose a plurality of fusible links to manifest said digital secret by permanently setting a binary state in each of said plurality of fusible links. However, Balard discloses a plurality of fusible links to manifest a digital secret by permanently setting a binary state in each of said plurality of fusible links, i.e. eFuse Array (paragraphs 44-45 and 101).

At the time applicant's invention was made, it would have been obvious to one skilled in the art to modify Okada's invention according to the limitations recited in claim 15 in light of Balard's teachings. One skilled would have been motivated to do so because storing a secret within a fuse array as per Balard's teachings would increase security for Okada's processor since any attempts at observing the secret would result in the destruction of the chip itself (Balard: paragraph 100), thus increasing security for Okada's invention.

Claim 16:

As per claim 16, Okada does not disclose wherein said digital secret comprises a random number that is generated from an HMAC algorithm implemented on testing data associated with fabrication of said IC chip. However, Balard discloses the limitation (Figures 2 and 10). It would have been obvious to one skilled in the art to modify Okada's invention according to the limitations recited in claim 16 in light of Balard's

teachings. One skilled would have been motivated to incorporate Balard's teachings for the same reasons given in claim 15.

Claim 17:

As per claim 17, Balard further discloses wherein said testing data comprises die test data (paragraph 42 and Fig 6). However, neither Okada nor Balard explicitly discloses testing data comprising wafer test data. However, official notice is taken that testing data comprises wafer test data was well known in the art at the time applicant's invention was made. It would have been obvious for one of ordinary skill in the art to include wafer test data within the combination invention of Okada and Balard as said testing data because testing a processor's wafer ensures quality of the processor.

Claim 20:

As per claim 20, Okada does not explicitly disclose wherein said key-based cryptography process comprises a triple data encryption algorithm (TDEA or Triple DES) cryptography process. However, Balard discloses use of triple DES (Fig 10, item 252). It would have been obvious to one skilled in the art to use triple DES as the key-based cryptography process in Okada's invention because triple DES offers a high level of security.

Claims 18-19 and 25-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Okada (US 6,704,872).

Claim 18:

Okada does not explicitly disclose that said secure cryptography unit comprises a fully integrated circuit within said processor. However, cryptographic units being implemented as fully integrated circuits were well known in the art at the time applicant's invention was made. It would have been obvious to one of ordinary skill in the art to modify Okada's invention according to the limitations recited in claim 18. One skilled would have been motivated to do so because use of an integrated circuit for the cryptography engine would result in faster encryption/decryption as cryptography implemented via hardware is typically faster than a software implementation.

Claim 19:

As per claim 19, Okada does not explicitly disclose that said digital secret and said internal memory are fully integrated within said cryptography engine to facilitate communication without requiring a bus and which is not susceptible to malicious attack. However, official notice is taken that functional units with integrated memory holding a secret key was well known in the art at the time applicant's invention was made. Because the components are integrated, a bus is not required for communication between the components. It would have been obvious to one of ordinary skill in the art to modify Okada's invention according to the limitations recited in claim 19. One skilled would have been motivated to do so because use of such an integrated circuit for the cryptography engine would make Okada's processor more secure.

Claim 25:

Claim 25 recites limitations substantially similar to what is recited in claim 18 and is rejected for the same reasons given therein.

Claim 26:

Claim 26 recites limitations substantially similar to what is recited in claim 19 and is rejected for the same reasons given therein.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 9:00am-4:30pm Mon-Thurs.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ponnoreay Pich
Examiner
Art Unit 2135

PP

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100